1.- OBJETIVO

Establecer las actividades técnicas, administrativas y organizativas que deben seguirse en el caso extraordinario de que un evento pudiera ocasionar que los sistemas fallen o se interrumpan, con menor o mayor impacto en su producción, manteniendo la continua ejecución de los procesos de misión crítica y sistemas de información tecnológica de la UADY; en caso de afectación, hacer eficiente la restauración de los sistemas que se hayan vuelto inoperables por el evento.

2.- ALCANCE

Aplica para todas las dependencias de la Universidad Autónoma de Yucatán que tengan a su cargo, o utilicen sistemas e infraestructura de tecnologías de información y comunicación.

3.- CONTENIDO

Plan de contingencias para Servicios Institucionales de TI

Contenido

I. Introducción

En la actualidad, los cambios tecnológicos adquieren cada vez mayor importancia al interior de las organizaciones; Por tanto, así como es necesario o indispensable contar con un plan de contingencias para los recursos tecnológicos, lo es también garantizar el restablecimiento de los servicios tecnológicos que ayuden a nuestro recurso humano a reanudar sus actividades en el menor tiempo posible.

Para incrementar la efectividad, mejorar la productividad, eficiencia del personal y proveer un servicio continuo y eficaz, los representantes de Seguridad de la Información de las Instituciones de Educación Superior (IES), hemos coincidido en que los activos de nuestras instituciones representan el elemento fundamental para la prestación de los servicios educativos y por ello, es importante la definición de lineamientos que favorezcan o propicien su uso racional, así como el desarrollo de procedimientos que garanticen la continuidad del servicio ante cualquier incidente.

Para cumplir con lo anterior, el Plan de Contingencias para Servicios Institucionales de TIC, representa una de las herramientas importantes ya que implica un análisis y evaluación riesgos a los cuales pueden estar expuestos los equipos de tecnologías de información y comunicación y, en consecuencia, la información contenida en los diversos medios de almacenamiento.

El Plan de Contingencias deberá incluir:

- Plan de recuperación de desastres, cuyo objetivo será restaurar los servicios de TIC en forma rápida, eficiente y con el mejor balance costo - beneficio.
- Plan de gestión de riesgos. Es sumamente importante definir, identificar las amenazas y vulnerabilidades que pueden afectar a la Institución. Podemos suponer que se pueden presentar diferentes niveles en la afectación, mínimo o total. Esto debe estar reflejado en el Plan de Contingencias.

Este Plan de Contingencia puede apoyar para crear un repositorio centralizado para la información, tareas y procedimientos que puedan ser necesarios para facilitar la toma de decisiones a la administración del IES, así como de desarrollar procesos y definir sus tiempos de respuesta ante cualquier falseo o interrupción extendida de las operaciones normales y servicios de la institución. Entendemos que estos riesgos pueden afectar a todo tipo de activos de la Institución:

- Personas
- Infraestructura / Instalaciones
- Información / Datos
- Tecnologías / Equipos
- Procesos / Actividades

Por ello es importante definir la causa de la interrupción para prevenir si una pronta restauración de las operaciones no pueda ser realizada empleando solamente procedimientos operacionales de un día normal.

En términos de personal y recursos financieros, las tareas de información y procedimientos detallados en este Plan demuestran a la administración del IES la importancia de contar con un plan de cómo responder, restaurar y recobrar. Por lo tanto, es esencial que la información y planes de acción de este plan, se mantengan viables y puedan ser mantenidos actualizados para poder asegurar la efectividad en el momento de su ejecución.

II. Organización

En el caso de un desastre u otra circunstancia que conlleve la necesidad de operaciones de contingencia, la organización normal de la UADY deberá cambiar a una organización de contingencia. La UADY deberá centrarse en cambiar la estructura actual y funciones de un "día normal de trabajo", a la estructura y funciones requeridas por la contingencia trabajando en conjunto para la restauración de los servicios institucionales de TIC.

III. Objetivos

3.1. Objetivo de un Plan de Contingencias:

El principal objetivo de un plan de contingencias considera la protección de los dos principales activos de una organización, el recurso humano y la información. Todas las facetas de un plan de contingencia deben responder a las amenazas latentes y, en consecuencia, orientar los esfuerzos a la protección y salvaguarda del personal, así como la protección y recuperación, si se requiere, de la información.

3.2. Objetivo General de Plan de Contingencias para Servicios Institucionales de TI:

Proporcionar a la UADY una herramienta que le permita garantizar el funcionamiento de la tecnología informática y su recuperación, en el menor tiempo posible.
Así, para tener la oportunidad de salvaguardar la integridad física del personal y asegurar la funcionalidad de los sistemas de información en caso de presentarse una contingencia, esta herramienta debe establecer las políticas, procedimientos y acciones oportunas que puedan apoyar los procedimientos de recuperación ante desastre.

Las medidas son, dependiendo de la variedad de sistemas clasificados,

- de función critica
- conectividad
- acceso a internet
- correo electrónico
- desarrollos propios de sistemas de bases de datos.

Con el Plan de Contingencia, tenemos mayor probabilidad de que la afectación a estos eventos (o vulnerabilidades en ellos) pueden ser mitigada, aunque en algunos no puedan ser prevenidos; sin embargo, para una IES, contar con este Plan es de relevancia para establecer procedimientos de recuperación de desastre para asegurar la continuidad del servicio a sus usuarios y/o clientes.

3.3. Objetivos Específicos:

Para cumplir con el objetivo general, es necesario

- Minimizar el número de decisiones que deben ser tomadas durante una contingencia
- Identificar los recursos necesarios para ejecutar las acciones definidas por este plan
- Identificar las acciones a ser tomadas por equipos previamente definidos
- Identificar información crítica, así como el responsable de recuperarla en las operaciones de restauración
- Definir el proceso para probar y mantener este plan y entrenamiento para equipos de contingencia de la organización

IV. Plan de contingencias y su estructura

El Plan de Contingencias es el instrumento de gestión para el buen manejo de las Tecnologías de la Información y Comunicación. Dicho plan contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad de las operaciones de la institución.

Asimismo, este Plan de Contingencias sigue la conocida metodología PDCA (Plan-Do-Check-Act), también conocido como ciclo Deming o ciclo Schewhart.

- Planificar
- Ejecutar
- Evaluar (Revisar)
- Actuar (Corregir)

Surge de un análisis de riesgos, donde, entre otras amenazas, se identifican aquellas que afectan a la continuidad de la operación de la institución. Como su nombre lo dice, es una secuencia cíclica que permite revisar las etapas del ciclo de vida de un producto o servicio e ir corrigiendo los fallos e implementando mejoras.

El plan de contingencias deberá ser revisado anualmente. Asimismo, es revisado/evaluado cuando se materializa una amenaza.

El plan de contingencias abarca cinco puntos importantes a través de sus diferentes secciones:

a) **Resguardo**. Contempla las medidas preventivas antes de que se materialice una amenaza. Su finalidad es evitar dicha materialización.

b) **Emergencias**. Contempla las medidas necesarias durante la materialización de una amenaza, o inmediatamente después. Su finalidad es contrarrestar los efectos adversos de la misma.

c) **Recuperación**. Contempla las medidas necesarias después de materializada y controlada la amenaza. Su finalidad es restaurar el estado de las cosas tal y como se encontraban antes de la materialización de la amenaza.

d) **Contingencias con huracanes**. Incorpora las acciones, responsables y actividades en caso de una amenaza de huracán.

e) **Contingencias con huelgas institucionales**. Incorpora las acciones, responsables y actividades en caso de una huelga académica o administrativa institucional.

El plan de contingencias deberá expresar claramente los siguientes tres aspectos:

a) **Qué recursos materiales son necesarios.**

Las instituciones deberán contar con un Centro de Respaldo Institucional (CRI), ya sea propietario o arrendatario.

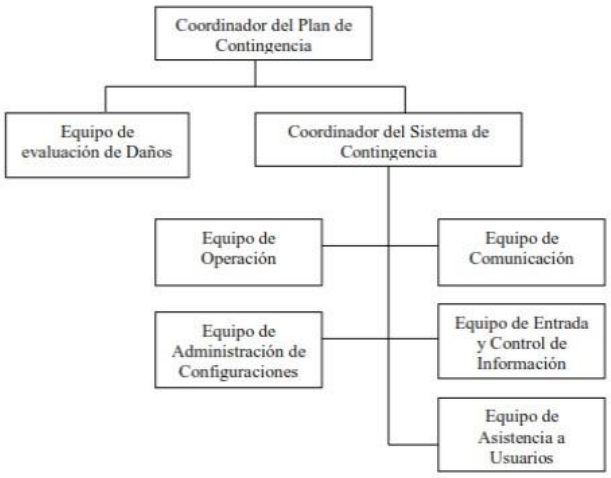
b) **Quienes están implicados en el cumplimiento del plan.** Cuales son sus responsabilidades concretas y su rol.

- Los Administradores de Tecnologías de Información (ATIs) de cada dependencia son los responsables de realizar todas las acciones relacionadas a los planes de contingencia, en cualquiera de sus tres sub-planes.
- Los ATIs deberán realizar todas las actividades establecidas en las políticas del reglamento de seguridad en coordinación con el responsable del CRI y con las áreas involucradas en materia de seguridad institucional.

c) **Acciones a seguir.**

- Determinar los requerimientos de los procesos del Centro de Proceso de Datos (CPD), verificando el análisis de riesgos y el análisis de impacto en él.
- Proveer procedimientos de recuperación para restaurar sus datos y servicios de procesamiento.
- Mantener y poner a prueba su solución de recuperación.

Una estructura propuesta es la que se presenta en el siguiente diagrama:



4.1. Fase de Contingencia

El Coordinador del Plan de Contingencia de la IES, en conjunto con sus directivos, deberá determinar cuáles equipos y miembros son responsables de cada función durante las fases:

a) Fase de Respuesta
b) Fase de Reasunción
c) Fase de Recuperación
d) Fase de Restauración

4.2. Sistemas/aplicaciones/servicios de misión critica

Los siguientes sistemas/aplicaciones/servicios de misión crítica deberán ser recuperados en el caso de un desastre:

Acrónimo del Sistema	Nombre Sistema
Conectividad LAN	*Conexión de Red Interna*
Conectividad WAN	*Conexión de Red Externa*
DNS	Servicio de Resolución de Nombres
Correo	Correo Electrónico Institucional
BD	Base de Datos Institucional

4.3. Amenazas

La siguiente tabla muestra las amenazas más comunes que podrían impactar la continuidad y componentes de sistemas y su administración.

Las amenazas que son presentadas con (XX) son consideradas las de mayor probabilidad de ocurrir.

Amenazas			
Probabilidad de Ocurrencia:	**Alta**	**Media**	**Baja**
Falla del aire acondicionado		***X***	
Accidente aéreo			***X***
Chantaje		***X***	
Amenazas de bomba			***X***
Frío / helada / Nieve			***X***
Perdida de comunicación		***X***	
Destrucción de información		***X***	
Terremotos			***X***
Fuego		***XX***	
Inundación / Daño por agua			***X***
Corte eléctrico / Interrupción	***XX***		
Sabotaje / Terrorismo			***X***
Tormentas / Huracanes		***X***	
Vandalismo		***X***	
Virus informáticos		***XX***	
Mal funcionamiento del equipamiento		***X***	
Personal que deja la institución (puede hacer mal uso de la información)		***X***	

V. Documentos necesarios previos a las contingencias

5.1 Documentos

1. Copia del inventario del mobiliario y equipo existente en el área.
   1.1. Comunicaciones
   1.2. Servidores
   1.3. Dispositivos de respaldo de energía
   1.4. Reguladores de voltaje
   1.5. Almacenamiento masivo (SAN, NAS)
   1.6. Dispositivos de entidades externas (Telmex, …)

2. Configuraciones del equipo de cómputo y telecomunicaciones que reside en el área.
   2.1. Determinar la información crítica y sacar respaldos de información de servidores, sobre todo, los que contengan base de datos
3. Documentación al día de contratos de mantenimiento de equipos e infraestructura.
   3.1. Listas de notificación
   3.2. Números de teléfono
   3.3. Mapas y direcciones
   3.4. Diagramas de TIC (datos, voz, eléctricos, …)
4. Protocolos de prioridades, responsabilidades, relaciones y procedimientos.

5. Sistemas, configuraciones y copias de seguridad en cinta.

VI. Plan para interrupción en el suministro de energía eléctrica de la CGTIC.

6.1 Acciones Preventivas a la Contingencia

6.1.1 Planta de Emergencia

- Contar con una planta de emergencia que suministre energía regulada, al menos, en cada Centro de Operaciones de la Red (NOC) y, recomendable, en los Centros de Distribución (Sites)
- Supervisar semanalmente el nivel óptimo de combustible, agua, baterías, etc.
- Contar con un plan de mantenimiento semestral con supervisiones mensuales.
- Supervisar el combustible de respaldo en el área de servicios generales.
- Contar con equipo de emergencia contra incendios en el local de la planta.
- Contar con el mapa eléctrico del área en la planta y archivado, identificando los contactos respaldados y regulados.
- Contar con un procedimiento de operación y uno en caso de un mal funcionamiento.
- Contar con tierras físicas independientes a los servicios de telecomunicaciones.

6.1.2 By Pass

- Contar con un *By Pass* en cada NOC o Site que contenga equipos críticos conectados a la red o al segmento de red
- Supervisar mensualmente el óptimo estado del *By Pass*.
- Contar con el mapa eléctrico del área ilustrando el *By Pass.*
- Plan de mantenimiento anual integral con supervisiones mensuales.

- Contar con un procedimiento de operación y uno en caso de un mal funcionamiento.
- Contar con los elementos necesarios para activar y/o desactivar el *By Pass.*

6.1.3 UPS

- Contar con UPS con capacidad suficiente para proporcionar tiempo de ejecución de procedimientos de apagado en condiciones de emergencia en todos los NOC o Sites
- Plan de mantenimiento anual integral con supervisiones mensuales.
- Contar con los diagramas eléctricos del área, identificando los contactos de energía.
- Contar con un procedimiento de operación y uno en caso de un mal funcionamiento.
- Determinar semestralmente el tiempo efectivo y real de respaldo del UPS con respecto a las diferentes cargas.

6.1.4 Generales

- Contar con la disponibilidad de, al menos, una línea telefónica (y teléfono) análoga activa en el NOC para utilizar en caso de emergencia que incluya la falla de energía eléctrica
- Disponibilidad de, al menos, una línea telefónica celular para apoyar las comunicaciones.
- Contar con un directorio de los responsables del suministro eléctrico en cada Campus, incluyendo de las IES.
- Contar con un procedimiento para reportar el incidente a las áreas involucradas
    - Servicios Generales
    - Telmex
    - CFE
    - Proveedores de Mantenimientos,
    - Etc.
- Contar con un procedimiento para notificar a los usuarios afectados la probable baja de los servicios de comunicación.

- Contar con procedimiento de ejecución de respaldos de emergencia a la información del servidor Web, Mail, DNS, configuraciones de Equipo Activo principales y centrales.
- Contar con una tabla de claves de prioridades para avisar a los usuarios prioritarios con el fin de optimizar tiempo y recursos.
- Solicitar revisión periódica (semestral) del estado y óptimo funcionamiento de los bancos de baterías en los equipos, con proveedor de la marca.
- Asignar jerarquía a los equipos Activos y Servicios para ejecutar medidas mayores (apagarlos).
    - Determinar las fases de una contingencia de esta índole
    - Tener la disponibilidad de material y herramientas necesarias:
        - Lámparas de emergencia
        - Impermeables
        - Cintas (canela, maskeen tape, de seguridad)
        - Pliegos de nylon o plástico sencillo y flexible para protección de los equipos, en caso necesario
        - Botas

6.2 Acciones Durante la Contingencia

6.2.1 En caso de interrupción del suministro eléctrico en lapsos cortos consecutivos:

- Comunicarse con servicios generales para la supervisión de la Planta de Emergencia.
- Monitorear el UPS cada 20 min. para programar acciones mayores.
- Valorar la decisión de apagar o desconectar los equipos activos y servicios para evitar daños y pérdida de información y de equipos.

6.2.2 En caso de una interrupción del suministro eléctrico no mayor a una hora:

- Comunicarse con servicios generales para la supervisión de la Planta de Emergencia.
- Monitorear el UPS cada 10 minutos para programar acciones mayores.
- Apagar los equipos no prioritarios como impresoras, monitores o PC que no demanden su uso.
- Desconectar electrodomésticos (cafeteras, equipo de sonido, refrigerador, horno de microondas, ventiladores, etc.).
- Contar con los procedimientos para dar de baja los equipos activos.
- Contar con radios de comunicación cargados.

6.2.3 En caso de una interrupción del suministro eléctrico mayor a una hora:

- Dar aviso de la contingencia a los usuarios prioritarios (Rectoría, Secretaría General, Finanzas y Administración, Desarrollo Académico, Planeación y Efectividad Institucional, CGTIC, Centros de Cómputo, Bibliotecas, Centros de Auto Aprendizaje, Institutos, Escuelas y Campus).
- Preparar el apagado de los equipos prioritarios (equipo activo).
- Comunicarse con servicios generales para la supervisión de la planta de emergencia con mayor énfasis
- Monitorear el UPS cada 5 minutos para programar acciones mayores.
- Dar de baja equipo activo y servicios con mediana prioridad con respecto a las fases definidas.

6.3 Acciones después de la Contingencia

- Brindar un tiempo de gracia (depende de la magnitud de la contingencia) para confirmar la estabilidad de la provisión de la alimentación eléctrica, y posteriormente proceder al restablecimiento los equipos activos y servicios.
- Restablecer los equipos activos y servicios que se dieron de baja, en forma paulatina.
- Validar el correcto funcionamiento de los equipos activos y servicios.
- Identificar los posibles daños de los equipos activos.
- Notificar a los usuarios afectados el restablecimiento de los servicios y su condición.
- Evaluar los daños de los equipos activos, planta de emergencia, UPS y canalizarlos a las áreas involucradas.

VII. Plan de contingencia para salvaguardar los expedientes del archivo de personal y control escolar.

7.1 **Contenido del plan de contingencia:**

a) Lista de números telefónicos de servicios auxiliares y de familiares del personal que labora en el área.

b) Prioridades, responsabilidades y procedimientos para el plan de contingencias.

c) Diagramas de instalaciones.

d) Copias de seguridad.

7.2 **Acciones preventivas a la contingencia (EXPEDIENTES)**

7.2.1 **INCENDIOS**

7.2.1.1 **Infraestructura**

a) La Coordinación General de Servicios Generales deberá contar con diagramas de las instalaciones; los responsables de cada área deberán contar con una copia.

b) Contar con extinguidores cargados.

c) Capacitación del personal para el uso adecuado de extinguidores por parte de servicios de bomberos.

d) Contar con señalamientos de rutas de evacuación.

e) Contar con lámparas emergentes con batería.

f) Realizar simulacros una vez por año en la dirección.

g) Contar con sistemas de alarmas.

7.2.1.2 **Servidores**

a) Contar con respaldos internos y externos.

b) Apagar servidores no prioritarios.

7.2.2 **HUMEDAD**

7.2.2.1 **Infraestructura**

a) Dar mantenimiento preventivo una vez por año con impermeabilizantes a los techos y paredes donde exista el riesgo de humedad.

b) Mantener ventilación en el área de archivo para evitar, alergias provocadas por la humedad (hongos).

c) Fumigar las áreas una vez por año para evitar la propagación de plagas como son las termitas, roedores, etc.

d) Colocar en lugares seguros y protegidos el hardware, software y documentos importantes.

e) Apagar equipos de cómputo prioritarios.

f) Contar con bolsas de plástico para cubrir servidores y documentos importantes que puedan dañarse con la humedad.

7.2.3 **ROBO O EXTRAVÍO**

7.2.3.1 **Infraestructura**

a) Colocar letreros o anuncios que impidan el acceso a personal no autorizado.

b) Que el personal autorizado cuente con identificación.

c) El lugar físico donde se encuentran resguardados los expedientes sea un lugar aislado y seguro.

7.2.3.2 **Servidores**

a) Evitar el acceso a personal no autorizado al área de servidores.

7.2.3.3 **Documentación**

a) Contar con formatos o bitácora de salida de expedientes autorizado por el jefe del área.
b) Vigilancia del personal que labora en el área de archivo.

7.3 **Acciones durante la Contingencia (EXPEDIENTES)**

7.3.1 **INCENDIOS**

7.3.1.1 **Infraestructura**

a) El director del área deberá contar con una copia de las instalaciones del área de trabajo.
b) Utilizar los extinguidores por personal capacitado.
c) Respetar los señalamientos de rutas de evacuación.
d) Mantener cargadas y en buen estado las lámparas de emergencia
e) Mantener en buen estado el sistema de alarmas contra incendios.

7.3.1.2 **Servidores**

a) Verificar que se tengan los respaldos externos
b) Apagar servidor.

7.3.2 **HUMEDAD**

7.3.2.1 **Infraestructura**

a) Abrir ventanas para mantener la ventilación en el área de archivo.
b) Colocar en lugares seguros el hardware, software y documentos importantes.
c) Apagar equipos de cómputo prioritarios.

7.3.2.2 **Servidores**

a) Cubrir con bolsas de plástico servidores y documentos importantes que puedan mojarse.

b) Colocar los *no-breaks* sobre mesas.

7.3.3 **ROBO O EXTRAVIO**

7.3.3.1 **Personal**

a) El personal que labora en el área deberá reportar el extravío o robo al jefe inmediato y en su caso a la dirección general jurídica para su investigación.

b) Tratar de localizar a la persona que extrajo el expediente.

7.3.3.2 **Documentación**

a) Buscar el formato de salida de expedientes autorizado por el jefe del área.

7.4 **Acciones después de la contingencia (EXPEDIENTES)**

a) Realizar un reporte de los daños.

b) Que el personal encargado del área de contingencia se reúna para analizar el plan de continencias y realizar las modificaciones correspondientes, así como las funciones o acciones del personal de contingencias.

VIII. Plan de contingencia para cuidar la integridad del personal

8.1 **Acciones antes de la contingencia**

a) Programar 2 simulacros al año.

b) Programar dos fumigaciones anuales, en periodos vacacionales.

c) Contar con botas e impermeables para poder entrar y salir de las instalaciones.

d) Conocer el manejo de los extintores.

e) Contar con batas, guantes y cubre bocas para el manejo del acervo.

f) Contar con botiquines de primeros auxilios en áreas estratégicas.

g) Contar con capacitación de primeros auxilios.

h) Implementar alarmas de emergencia en lugares estratégicos dentro de las instalaciones.

i) Establecer puntos de reunión dentro y fuera de las instalaciones.

j) Difundir las rutas de evacuación, así como los sitios de localización de alarmas, extintores.

k) Establecer procedimientos de evacuación.

l) Capacitación permanente y actualizada a los comités de Seguridad e Higiene y al de Seguridad en Cómputo.

m) Contar con un directorio del personal.

8.2 **Acciones durante la contingencia**

a) Accionar las alarmas de emergencia.

b) Utilizar las botas e impermeables para poder salir o ingresar a las instalaciones en caso de inundación.

c) Dirigir a los usuarios en la evacuación e información de salidas de emergencia.

d) Priorizar la evacuación.

e) Llamar al 911.

8.3 **Acciones después de la contingencia**

a) Brindar los primeros auxilios a las personas que lo requieran.

b) Realizar un recuento de los daños causados.

c) Realizar un informe con los hallazgos y emitir a la Dirección.

d) Tomar acciones de acuerdo con el informe emitido.

e) Retroalimentar los planes de contingencia con la experiencia de contingencias anteriores.

IX. Plan de contingencias para Fenómenos Meteorológicos Extremos (CGTIC)

9.1 **Acciones preventivas.**

En caso de Huracán o tormenta tropical, seguir las siguientes medidas de prevención:

9.1.1 **Infraestructura**

a) Mantener llenos los tanques de gasolina de los automóviles. Los vales pueden ser solicitados al Coordinador General.

Responsable: jefes de departamento

b) Realizar mantenimiento general de la planta eléctrica de emergencia.

Responsable: Emmanuel Serrano

c) Mantener el tanque de la planta de emergencia lleno de diesel.

Responsable: Emmanuel Serrano

d) Tener un tambo de Diesel lleno.

Responsable: Sergio Cervera

e) Comprar pilas para lámpara de emergencia.

Responsable: Ángel Arroyo.

f) Coordinar el servicio de impermeabilizante a los techos y/o paredes.

Responsable: Sergio Cervera

g) Contar con agua purificada suficiente (Mínimo, 5 garrafones)

Responsable: Sergio Aguilar

h) Contar con impermeables.

Responsable: Sergio Aguilar

i) Encintar ventanas y sellar puerta trasera y delantera de la coordinación donde se pueda filtrar agua.

Responsable: jefes de departamento

j) Tener a la mano el mapa eléctrico de la Coordinación.

Responsable: Carmen Díaz

9.1.2 **Equipos de Telecomunicaciones**

a) Mantenimiento anual de mayo a junio de las torres de comunicaciones. Enlistar por DES instalaciones vulnerables.

Responsable: Israel Novelo

b) Aislar equipos que estén en riesgo, p.e., en el piso.

Responsable: Israel Novelo

9.1.3 **Servidores**

a) Sacar relación de servicios prioritarios: DNS, correo electrónico, Real Audio, Web, Citrix e Internet.

Responsable: Israel Novelo

b) Apagar Servidores no prioritarios

Responsable: Wilberth Pérez / Israel Novelo

c) Tapar con bolsas de plástico servidores que pueden mojarse

Responsable: Wilberth Pérez / Israel Novelo

d) Poner sobre mesas los no-breaks de servidores

Responsable: Wilberth Pérez / Israel Novelo

e) Generar los últimos respaldos

Responsable: Wilberth Pérez / Israel Novelo

f) Poner en un lugar distante los respaldos de información

Responsable: Angel Arroyo

9.1.4 **Telecomunicaciones**

a) Sacar relación de equipos prioritarios

Responsable: Emmanuel Serrano

b) Apagar equipos no prioritarios

Responsable: Emmanuel Serrano / Carlos Rico

c) Tapar con bolsas de plástico equipos de comunicaciones que pueden mojarse.

Responsable: Emmanuel Serrano / Fernando Osorno

d) Poner sobre mesas los no-breaks de equipos de comunicaciones

Responsable: Wilberth Pérez / Israel Novelo

e) Generar respaldos de configuraciones e imprimirlos

Responsable: Enrique Solís

9.1.5 **Servicios de Información**

a) Contar del mes de junio al mes de octubre con una liga permanente hacia Centros de Información de Huracanes.

Responsable: Enrique Solís

c) En caso de amenaza de Huracán, dejar liga sobre el estado del fenómeno e información de servicio a la comunidad: albergues, teléfonos de emergencia, etc.

Responsable: Enrique Solís

d) Enviar comunicado a los Directivos y ATI's sobre plan de contingencia y emergencia, indicando números disponibles para reportes y soporte. Responsable: Sergio Cervera

e) Coordinador General y Responsables de área: contar con computadora portátil con carga en pila para estar pendientes de los servicios de la RIUADY en caso de emergencia.

Responsable: Sergio Aguilar

f) Tener disponibles los números telefónicos del personal de la Coordinación General y de los responsables de redes de las dependencias universitarias.

Responsable: Sergio Aguilar

g) Contar una línea telefónica analógica con dispositivo analógico.

Responsable: Ángel Arroyo

h) Tener los celulares cargados.

Responsables: Todos

i) Imprimir hojas de reporte para llevar control de reportes por escrito.

Responsable: Sergio Aguilar

9.2 **Durante la Contingencia**

9.2.1 **Infraestructura**

a) Si la planta se encuentra en funcionamiento no se deberán conectar equipos con motor como refrigerador y no se proporcionará el servicio de carga de teléfonos celulares.

Responsable: Sergio Aguilar

b) Contar con mangueras y embudo para poner diesel, llevando extinguidor por si se requiere.
Responsable: Se irán turnando: Israel Novelo, Emmanuel Serrano, Ángel Arroyo, Marco Cervera, Enrique Solís, Wilberth Pérez, Sergio Aguilar.

c) En caso de que la planta haya trabajado más de 72 horas sin parar, se recomienda hablar a proveedor para mantenimiento.

Responsable: Emmanuel Serrano

9.2.2 **Telecomunicaciones**

a) Verificación de enlaces hacia Internet y servidores, paulatinamente verificación de enlaces a

DES, generando relación de los que ya están en funcionamiento.
Responsable: jefes de departamento con apoyo de mesa de
servicios.

b) Verificación de estado de los equipos y secado de los mismos en caso necesario
Responsable: Israel Novelo / Carmen Díaz, con apoyo de jefes de departamento

c) Levantamiento de reportes de DES con problemas y establecimiento de prioridades para atención.

Responsable: Israel Novelo / Carmen Díaz, con apoyo de mesa de servicios.

9.2.3 **Servidores**

a) Verificación de servicios prioritarios de la RIUADY.
Responsable: Israel Novelo / jefes de departamento

b) Verificación de estado de los equipos y secado de los mismos en caso necesario.
Responsable: Israel Novelo / jefes de departamento

c) Levantamiento todos los servicios adicionales.
Responsable: Israel Novelo / jefes de
departamento

9.3 **Apoyo que brinda el área de Gestión**

9.3.1 **Recursos**

a) Verificación de la disponibilidad de recursos financieros, para que, en caso de ser necesario, se efectúe la compra de material o artículos de emergencia.

b) Coordinar al personal que participará en la realización de acciones preventivas y actividades durante la contingencia.

c) Supervisar que el personal cumpla adecuadamente con las labores de apoyo que se requieran ante la contingencia.

9.3.2 **Notificación a Funcionarios de las Dependencias y ATIs**

Estimados Directores y Administradores de Tecnologías de Información de la UADY:

Como parte del proceso para “Diseño y Provisión de Tecnologías de Información” de nuestro Sistema de Gestión de Calidad Institucional y ante la temporada de Huracanes 2012 que inició el 1ro. de junio del presente, es recomendable adoptar un Plan de Contingencia que permita, en lo posible, dejar en buen resguardo la infraestructura de nuestra Institución, minimizando los efectos que se pudiesen presentar.

Anexo al presente encontrarán el Plan correspondiente a la RIUADY (esta información también está publicada en el portal de internet de la RIUADY: http://www.riuady.uady.mx/)

Así mismo se estarán actualizando los boletines emitidos por el comité institucional de protección civil.

En este sitio encontrarán información actualizada de los niveles de alerta de nuestro estado emitido por el Gobierno del Estado de Yucatán, así como una liga al Centro de Huracanes de Miami (NOAA), http://www.uady.mx/universidad/huracanes.html.

Esperando que esta información les sea de utilidad, quedo de ustedes.

Atentamente

Coordinación General de Tecnologías de Información y comunicación (CGTIC)

X. Plan de contingencias para Fenómenos Meteorológicos Extremos (DES)

10.1. Etapa de PREVENCIÓN, Alerta Azul.

10.1.1. Acciones

a) Copia del inventario del mobiliario y equipo existente en el área de T.I.

b) Listado de configuraciones del equipo de cómputo y telecomunicaciones que reside en el área.

c) Documentación al día de contratos de mantenimiento de infraestructura.

d) Listas de notificación, números de teléfono, mapas y direcciones.

e) Prioridades, responsabilidades y procedimientos.

f) Información sobre adquisiciones y compras.

g) Diagramas de las instalaciones, Sistemas, configuraciones y copias de seguridad, en cinta o Servicio de la Nube.

h) Determinar la información crítica y sacar respaldos de información de la Dependencia de Educación Superior (DES).

i) Tener impreso los directorios del personal de emergencia (proveedores y personal de la CGTIC). j) Contar con impermeables.

10.1.2. DES que cuentan con Planta de Emergencia:

a) Realizar mantenimiento general de la planta eléctrica de emergencia.

b) Mantener tanque lleno de diesel.

c) Tener un tambo o bidón de diesel lleno.

10.1.3. DES que cuentan con Enlaces Inalámbricos:

a) Realizar mantenimiento general del enlace inalámbrico, incluyendo la torre de comunicaciones.

b) Verificar la vigencia de póliza de los radios que proporcionan el servicio inalámbrico.

10.2. Etapa de PREVENCIÓN, Alerta Amarilla.

a) Alejar los equipos de las ventanas o de alguna posible entrada de viento o agua.

b) Verificar el funcionamiento de servicios de acceso remoto, tales como: Infinitum de DES, Citrix, VPNs, en su caso.

c) Sacar los respaldos de información de la DES.

d) Contar una línea telefónica analógica con dispositivo analógico, en su caso conectar un teléfono analógico en la línea ISDN de su DES.

e) Tener los teléfonos celulares cargados.

f) Revisar instalaciones expuestas a vientos como torres, antenas, letreros, etc.

10.3. Etapa de PREVENCIÓN, Alerta Naranja.

a) Contar con impermeables, lámparas de emergencia, jergas, cinta.

b) Ponerse en comunicación con la Coordinación General de Tecnologías de Información y Comunicación, para coordinar el apagado de los Equipos.

c) Apagar y desconectar equipos de cómputo y comunicaciones, incluyendo *no-breaks*.

d) Colocar los equipos, incluyendo los *no-breaks* sobre mesas.

e) Encintar ventanas.

f) Cubrir los equipos con bolsas de plástico.

g) Resguardar todo tipo de expediente en zonas seguras, libres de inundaciones, goteras y filtraciones.

h) Llenar los tanques de los vehículos con combustible.

10.4. Etapa de RECUPERACIÓN, posterior al Fenómeno Meteorológico Extremo (DES).

a) Revisión de daños en las ventanas del centro de comunicaciones, centro de cómputo y/o áreas correspondientes. En su caso aislar los equipos afectados o en amenaza. Limpiar y secar pisos.

b) Verificar el funcionamiento de las líneas telefónicas.

c) Secar los equipos *no-breaks* antes de encenderlos a fin de evitar que exploten por exceso de humedad; en lo posible con compresor de aire.

d) Secar los equipos de comunicaciones y posteriormente verificar que los equipos estén en funcionamiento.

e) En caso de contar con enlace inalámbrico, verificar posibles daños en la infraestructura de torre de comunicaciones.

f) Ponerse en comunicación con la Coordinación General de Tecnologías de Información y Comunicación, para coordinar el Inicio de los Equipos y Servicios.

Ponemos a su disposición los números telefónicos de la Coordinación General de Tecnologías de Información y Comunicación.

Teléfono: 9999237428

Celulares:

Carmen Díaz 9992 654940

Israel Novelo 9992 384079

XI. Políticas de continuidad de los servicios en caso de una huelga

a) Respaldos de información crítica de los servicios institucionales.

b) Establecimiento de instalaciones alternas (fuera de la institución) con acceso a internet para los siguientes procesos:

- Nomina institucional.
- Sistema Institucional de Información
- Servicio Médico para el Personal de la Universidad en apoyo a la Coordinación General de Salud.
- Procesos de Adquisición Institucional
- Sistema Institucional de Control Escolar
- UADY Virtual

c) Establecimiento y activación de un Call Center.

d) Difusión de Comunicados a través del Portal Institucional.

e) Continuidad de actividades académicas a través de la plataforma UADY Virtual.
f) Implementación de servicios institucionales en la Nube de Internet de la UADY. g) Soporte remoto y en sitio a usuarios de los procesos institucionales.

h) Capacitación a demanda de herramientas de trabajo colaborativo.

4.- DOCUMENTOS DE REFERENCIA

Código	Nombre del documento	Lugar de almacenamiento
L-SG- CGTIC-03	Código de Conducta	Sitio Web de Calidad
L-SG- CGTIC-04	Políticas Institucionales de Seguridad en Cómputo	Sitio Web de Calidad

5.- GLOSARIO

5.1 .- SIGLAS

ATI: Administrador de Tecnologías de Información.

CGTIC: Coordinación General de Tecnologías de información y Comunicación.

DES. Dependencia de Educación Superior de la UADY.
RIUADY. Red Integral de la Universidad Autónoma de Yucatán
SAU: Sistema de Atención a Usuarios

SG: Secretaría General

TIC: Tecnologías de Información y Comunicaciones

5.2 .- DEFINICIONES

Aplicaciones críticas. Aplicaciones utilizadas por usuarios de todas las Dependencias y Facultades o aquellas que proveen servicios de seguridad y acceso.

Base de conocimientos. Instructivos: Conjunto de instructivos utilizados en la CGTIC para la atención de los servicios.

Becario. Estudiante de una institución de educación superior, de áreas de conocimiento afines a las TI, que se encuentra en proceso de capacitación para atender las solicitudes y reportes del sistema de atención a usuarios.
Gestión de TI. Área de la CGTIC responsable del cumplimiento administrativo de los servicios de TI.

Intranet: Conjunto de servidores y servicios donde se encuentran alojados los sistemas de TI de la CGTIC.

Mesa de Servicio. Personal o Becario de la UADY asignado a una o varias áreas de la CGTIC y que apoya en las actividades técnicas necesarias para la atención de los servicios de TI. Realiza el primer contacto con el usuario.

Servidor crítico. Servidor donde se ejecutan una o varias aplicaciones críticas

Servidor no crítico. Servidor donde se ejecutan aplicaciones que no son críticas.

Jefe de departamento. Especialista de TI, responsable de instruir, orientar y dar seguimiento a las actividades del personal de la mesa de servicio que está asignado a su área en la CGTIC.

Usuario. Es el personal académico, personal administrativo, alumnos, alumnos potenciales, administradores de tecnologías de información de la UADY, así como personas de otras IES, usuarios comerciales, gobierno y sociedad que requieren de los servicios de tecnologías de información ofrecidos por la CGTI

6.- CONTROL DE REVISIONES

Nivel de revisión	Sección y/o página	Descripción de la modificación y mejora	Fecha de modificación
01	Todo	Integración del documento al de SGC.	15 de junio 2016
02	Todo	Cambio de siglas a CGTIC	22 de septiembre de 2019

Nota: Ésta sección será utilizada a partir de la primera modificación a este documento. La revisión 00, se mantendrá en blanco.

Revisó	**Aprobó**
MATI. Israel Novelo Zel	*MT Sergio Antonio Cervera Loeza*
Coordinador de Infraestructura Tecnológica de la CGTIC	*Coordinador General de Tecnologías de la Información y Comunicación*